COMPLIANCE CHECKLIST

SOC 2 compliance checklist

Service Organization Control 2 (AICPA attestation standards - AT-C 105 and AT-C 205, as amended through SSAE No. 23 effective for engagements beginning on or after 15 December 2025)

Jurisdiction: US service organisations (global by reciprocal trust)

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who SOC 2 applies to

Technology service organisations that hold or process customer data and want to demonstrate trust through an independent AICPA-aligned report. Not a regulatory requirement - a market-driven standard.

SOC 2 checklist

STEP 1

- [ ] Select the Trust Service Criteria - Security (mandatory) plus optional Availability, Confidentiality, Processing Integrity, or Privacy.

STEP 2

- [ ] Decide between SOC 2 Type I (design at a point in time) or Type II (operating effectiveness over 6-12 months).

STEP 3

- [ ] Inventory in-scope systems and document the system description per AICPA guidance.

STEP 4

- [ ] Map controls to the chosen TSC criteria and identify owners for each.

STEP 5

- [ ] Engage an AICPA-licensed CPA firm and complete a readiness assessment.

STEP 6

- [ ] Remediate gaps from readiness and operate controls for the audit window (Type II).

STEP 7

- [ ] Gather evidence throughout the audit window - screenshots, tickets, system reports.

STEP 8

- [ ] Auditor performs fieldwork: inquiry, inspection, observation, re-performance.

STEP 9

- [ ] Receive the SOC 2 report - opinion, system description, criteria, controls, tests, results.

STEP 10

- [ ] Distribute the report under NDA to customers and prospects under your established sharing policy.

FAQ

Type I or Type II?

Type I attests to control design at a point in time. Type II attests to operating effectiveness over a period (typically 6-12 months). Customers and procurement teams overwhelmingly expect Type II; Type I is most useful as an interim milestone for first-time auditees.

What are the Trust Service Criteria?

The five TSC are Security (Common Criteria - mandatory), Availability, Confidentiality, Processing Integrity, and Privacy. Most SOC 2 reports cover Security + one or two others depending on the service. Adding more criteria expands scope and audit cost.

How long does SOC 2 readiness take?

For most companies, 3-6 months from readiness assessment to a Type II audit window opening, then 6-12 months of operating before the auditor reports. Compressing the operating window is the single biggest constraint on calendar time.

Is SOC 2 the same as ISO 27001?

Both demonstrate information-security maturity, but they're different artefacts. ISO 27001 is a certification (yes/no, with a 3-year cycle); SOC 2 is an examination performed under the AICPA's attestation standards (AT-C 105/205) producing an opinion plus detailed evidence. Many service organisations carry both - ISO 27001 for European procurement, SOC 2 for North American.

Source: https://ba-copilot.com/compliance/soc-2-compliance-checklist. Tick each item as it is completed and add the named owner.